613-001980 Rev.A 140619

CentreCOM® *x510* シリーズ・*AT-IX5-28GPX* リリースノート

この度は、CentreCOM x510 シリーズ、AT-IX5-28GPX をお買いあげいただき、誠にありがとうございます。このリリースノートは、取扱説明書、コマンドリファレンスの補足や、ご使用の前にご理解いただきたい注意点など、お客様に最新の情報をお知らせするものです。
最初にこのリリースノートをよくお読みになり、本製品を正しくご使用ください。

1　ファームウェアバージョン　5.4.3-3.12

2　重要：注意事項

2.1　ファームウェアバージョンアップ時の注意事項

AT-x510-28GPX、AT-x510-52GPX、AT-IX5-28GPX をファームウェアバージョン 5.4.3-3.9 以降に更新後、最初の起動時には、必要に応じて PoE チップのソフトウェア更新が行われるため、起動時間が通常より 30 秒程度長くなる可能性があります。

3　本バージョンで追加・拡張された機能

ファームウェアバージョン **5.4.3-3.9** から **5.4.3-3.12** へのバージョンアップにおいて、以下の機能が追加・拡張されました。

3.1　Group-specific クエリーのフラッディング抑止設定

参照「コマンドリファレンス」/「IP マルチキャスト」/「IGMP」

IGMP/IGMP Snooping の Querier 機能において、Group-Specific Membership Query をフラッディングせずに、該当グループのメンバーが存在するポートにだけ送信させるオプションが追加されました。初期設定ではフラッディングしますが、新しく追加された ip igmp flood specific-query コマンドを no 形式で実行することにより、メンバーが存在するポートにだけ送信するようになります。

3.2　未登録マルチキャストグループの保持時間設定

参照「コマンドリファレンス」/「IP マルチキャスト」/「IGMP Snooping」

IGMP Snooping において、未登録マルチキャストグループの保持時間を設定する ip igmp snooping source-timeout コマンド（グローバルコンフィグモード）、ip igmp snooping source-timeout コマンド（インターフェースモード）、show ip igmp snooping source-timeout コマンドをサポートしました。

ip igmp snooping source-timeout コマンド

モード

グローバルコンフィグモード

書式

```
ip igmp snooping source-timeout <0-86400>
```

```
no ip igmp snooping source-timeout
```

解説

IGMP Snooping において、マルチキャストトラフィックの受信によって生成される未登録マルチキャストグループのエントリー保持時間を、IGMP Report の受信によって生成される通常のマルチキャストグループとは別に設定する機能を有効化する。
no 形式で実行した場合は本機能を無効化し、未登録マルチキャストグループに対して通常のマルチキャストグループと同じ保持時間を適用する。
初期設定は無効。
なお、インターフェースモードの ip igmp snooping source-timeout コマンド（インターフェースモード）で VLAN インターフェース固有の設定がなされている場合、該当 VLAN においては、本コマンドの全体設定ではなく VLAN 固有設定が使用される。VLAN 固有の設定がされていない場合は、本コマンドの全体設定が使用される。

パラメーター

<0-86400>
未登録マルチキャストグループの保持時間。0 は無期限に保持する（削除しない）ことを意味する。

注意・補足事項

・本コマンドを 0 に設定している場合、未登録マルチキャストグループを削除するには clear ip igmp コマンドを使う。

・本コマンドの設定は、本コマンドの実行後に生成されるエントリーにだけ影響し、既存のエントリーには影響しない。本コマンドの設定をすべてのエントリーに適用したい場合は、clear ip igmp コマンドで既存エントリーをいったん削除すること。

・本コマンドは、マルチキャストトラフィックの送信者だけが存在し、受信者は存在しないネットワークでのみ使用可能。マルチキャスト受信者（IGMP ホスト）の存在するネットワーク（インターフェース）では使用しないこと。

ip igmp snooping source-timeout コマンド

モード

インターフェースモード

書式

```
ip igmp snooping source-timeout <0-86400>
```

```
no ip igmp snooping source-timeout
```

解説

対象 VLAN インターフェースにおける、IGMP Snooping の未登録マルチキャストグループ保持時間を設定する。
no 形式で実行した場合は対象 VLAN インターフェース固有の保持時間設定を削除する。
初期状態は未設定。
本コマンドで設定した VLAN インターフェース固有の保持時間は、ip igmp snooping source-timeout コマンド（グローバルコンフィグモード）による全体

設定よりも優先される。本コマンドが設定されていない VLAN では、全体設定が使用される。

パラメーター

<0-86400>
未登録マルチキャストグループの保持時間。0 は無期限に保持する（削除しない）ことを意味する。初期状態では VLAN インターフェース固有の保持時間は設定されていないため、全体設定（ip igmp snooping source-timeout コマンド（グローバルコンフィグモード））が使用される。

注意・補足事項

・本コマンドを 0 に設定している場合、未登録マルチキャストグループを削除するには clear ip igmp コマンドを使う。

・本コマンドの設定は、本コマンドの実行後に生成されるエントリーにだけ影響し、既存のエントリーには影響しない。本コマンドの設定をすべてのエントリーに適用したい場合は、clear ip igmp コマンドで既存エントリーをいったん削除すること。

・本コマンドは、マルチキャストトラフィックの送信者だけが存在し、受信者は存在しないネットワークでのみ使用可能。マルチキャスト受信者（IGMP ホスト）の存在するネットワーク（インターフェース）では使用しないこと。

show ip igmp snooping source-timeout コマンド

モード

非特権 EXEC モード

書式

```
show ip igmp snooping source-timeout
```

解説

IGMP Snooping における未登録マルチキャストグループ保持時間の設定を表示する。

使用例

```
awplus> show ip igmp snooping source-timeout ?
Global IGMP snooping source-timeout is disabled

vlan1            enabled (0 secs)
vlan2            disabled
```

4　本バージョンで修正された機能

ファームウェアバージョン **5.4.3-3.9** から **5.4.3-3.12** へのバージョンアップにおいて、以下の項目が修正されました。

4.1　AT-x510DP-52GTX と AT-IX5-28GPX において、電圧監視機能の最小しきい値が動作していませんでしたが、これを修正しました。

4.2 AT-x510DP-52GTX と AT-IX5-28GPX において、SFP+ モジュール装着時に関連プロセスでメモリーリークが発生することがありましたが、これを修正しました。

4.3 watchdog タイマーが満了し再起動することがありましたが、これを修正しました。

4.4 TFTP サーバーへのリモートコピー（アップロード）時、Write Request パケットで送信するファイル名の先頭に余分なスラッシュ（/）を付加していたため、TFTP サーバーによっては転送に失敗することがありましたが、これを修正しました。

4.5 PoE 対応機種（AT-x510-28GPX, AT-x510-52GPX）と非対応機種（AT-x510-28GTX, AT-x510-52GTX, AT-x510-28GSX）が混在する VCS 構成において、PoE 対応機器がダウンして VCS グループ内に PoE 対応機器が存在しなくなると、ランニングコンフィグ上から service inline コマンドが削除されていましたが、これを修正しました。

4.6 show tech-support コマンドによって内部的に実行されたコマンド操作は、TACACS+ サーバーにコマンドアカウンティングメッセージとして送信されませんでしたが、これを修正しました。

4.7 show trigger コマンドに counter パラメーターを指定した際に表示されるトリガーの統計情報に不適切な項目がありましたが、これを修正しました。

4.8 NTP 脆弱性（JVNVU#96176042）への対策を行いました。

4.9 show platform port コマンドにおいて、SFP+ ポートの Jam 状態が正しく表示されませんでしたが、これを修正しました。

4.10 スイッチポートにポリシーマップを適用した状態で Web 認証を有効化すると、関連プロセスが異常終了することがありましたが、これを修正しました。

4.11 HTTP リダイレクト機能とセッションキープ機能を有効にしている状態で、Windows 7 の端末から Web 認証画面にアクセスすると、システムがリブートすることがありましたが、これを修正しました。

4.12 2 ステップ認証とクリティカルポートを併用している認証ポートにおいて、1 つ目の認証で RADIUS サーバーが無応答でも、同認証をパスせず、2 つ目の認証に移行しませんでしたが、これを修正しました。

4.13 2 ステップ認証とクリティカルポートを併用している認証ポートにおいて、特定の Supplicant に対する「port-control skip-second-auth」（2 つ目の認証を行わない）設定が機能しませんでしたが、これを修正しました。

4.14 ポート認証において、Supplicant の通信中に VCS マスター切り替えが発生すると、マスターとスレーブの間で認証情報の不整合が生じ通信できなくなることがありましたが、これを修正しました。

4.15 ポート認証で Supplicant がログアウトしても、FDB から該当 Supplicant のエントリーが削除されず、通信が遮断されませんでしたが、これを修正しました。

4.16 802.1X 認証と Web 認証の 2 ステップ認証とクリティカルポートを併用した場合、2 回目以降の Web 認証が自動で行われてしまうことがありましたが、これを修正しました。

4.17 switchport trunk allowed vlan コマンドに except パラメーターを指定した場合、まれに ARP 応答などが正しく行われなくなることがありましたが、これを修正しました。

4.18 トランクポートに設定された所属先タグ VLAN を switchport trunk allowed vlan コマンドを使用して削除した場合、この VLAN 宛の通信が停止してしまうことがありましたが、これを修正しました。

4.19 RSTP/MSTP 使用時、スイッチがプロポーザルフラグを持つ BPDU を繰り返し受信する特殊な環境において、通信ができなくなることがありましたが、これを修正しました。

4.20 UDP ブロードキャストヘルパー機能の設定を削除した際に、コンフィグ関連プロセスが異常終了する場合がありましたが、これを修正しました。

4.21 OSPFv3 隣接ルーターとして Cisco 製ルーターを使用している場合、VCS マスター切り替え後の隣接機器との同期に時間がかかっていましたが、これを修正しました。

4.22 OSPFv3 でルートマップを使ってスタティック経路を再配信すると、LSDB にコストが 0 として登録されていましたが、正しいコストが登録されるよう修正しました。

4.23 短時間で多数のマルチキャストグループの参加・脱退を繰り返すと、参加後に全てのグループのマルチキャストが回復するのに時間がかかることがありましたが、これを修正しました。

4.24 IGMP Snooping が無効の場合、プライオリティーの高い Querier で show ip igmp interface コマンドの IGMP querying router is が正しく表示されませんでしたが、これを修正しました。

4.25 IGMPv2 のパケット（Report、Leave）や、IGMPv3 のパケット（Change_To_Exclude、Change_To_Include）を受信したときに、「Failed to find real Src-Rec from a Clone!」、「Invalid Rexmit HRT」のログが大量に表示されることがありましたが、これを修正しました。

4.26 IGMP や MLD などの CPU 宛のパケットを大量に受信している間、レジリエンシーリンクのヘルスチェックが失敗と成功を繰り返していましたが、これを修正しました。

4.27 CHANGE_TO_INCLUDE IGMP/MLD メッセージを受信した時に「Rexmit failed」というログが warning レベルで出力されていましたが、informational レベルで出力されるよう変更しました。

4.28 AMF で手動リカバリーを行う際、最新のバックアップデータを持つマスターの検出に失敗することがありましたが、これを修正しました。

4.29 ワーキングセットプロンプトでは、各種 show コマンドの出力に対してモディファイア（| include）が機能しませんでしたが、これを修正しました。

4.30 VCS 構成において、独自の SSL サーバー証明書をインストール、削除後に、Web 認証サーバーの HTTPS（SSL）機能を有効にすると、スタックメンバーが再起動することがありましたが、これを修正しました。

4.31 OSPFv3 使用時にリブートローリングを実施した場合、VCS マスター切り替えの際の IPv6 トラフィックの切断時間が通常より長くなっていましたが、これを修正しました。

4.32 VCS 構成時にトランクグループ上でダイナミック VLAN とゲスト VLAN を併用している場合、VCS メンバーが加入すると認証ポートの VLAN ID が誤った値に変更されていましたが、これを修正しました。

4.33 Disabled Master Monitoring 機能において、Disabled Master から Active Master に状態遷移すると、IPv6 通信ができなくなっていましたが、これを修正しました。

4.34 複数の VCS メンバーが同時に再起動した場合、コンフィグファイルが大きすぎると起動に失敗することがありましたが、これを修正しました。

下記の項目は、ファームウェアバージョン 5.4.3-3.7 のリリースノート、5.4.3-3.9 のリリースノートに制限事項として記載されていましたが、実際には 5.4.3-2.5 で修正されていました。

4.35 banner exec コマンドを no 形式で入力したコンフィグが実行されている場合、Web GUI にログインすることができませんでしたが、これを修正しました。

5　本バージョンでの制限事項

ファームウェアバージョン **5.4.3-3.12** には、以下の制限事項があります。

5.1　システム

参照「コマンドリファレンス」/「運用・管理」/「システム」

○　次の通常起動時にロードされる通常用ファームウェアのイメージファイルが USB メモリー上にある状態で VCS のスタックメンバーに加入し、そのファームウェアが VCS マスターのものと異なると、次の緊急起動時にロードされるバックアップ用ファームウェアのイメージファイルが、USB メモリーではなくフラッシュメモリーにあるものとして指定されてしまいます。

○　本製品は SD カードには対応していませんが、USB オートブート時に、SD カードに関するエラーメッセージがログに出力されます。これは表示のみの問題であり、動作には影響しません。

・　daemon.err awplus automount[2577]: failed to mount /mnt/card

○　reboot/reload コマンドで stack-member パラメーターを指定した場合、確認メッセージが表示されますが、ここで Ctrl/Z や Ctrl/C を入力した場合はその後 Enter キーを入力してください。Ctrl/Z や Ctrl/C を入力しただけではコマンドプロンプトに戻りません。

○　省電力イーサネット機能（ecofriendly lpi コマンド）を有効にした状態で VCS マスターを繰り返し再起動させると、VCS の同期が完了した後、同機能が無効になります。

○ USB メモリーを挿入したまま起動すると、LED が点灯・点滅しません。USB メモリーは起動後に挿入しなおしてください。

○ no ip domain-lookup コマンドを実行する以前に、1 度でも ntp server コマンドの設定を行ってしまうと、no ip domain-lookup コマンドを実行したとしても DNS へ問い合わせを行ってしまいます。trigger コマンドで再起動時に no ip domain-lookup コマンドが ntp server コマンドより先に実行されるように設定することにより、no ip domain-lookup の機能が正常に動作します。

5.2 コマンドラインインターフェース（CLI）

参照 「コマンドリファレンス」/「運用・管理」/「コマンドラインインターフェース」

edit コマンドを使用すると、コンソールターミナルのサイズが自動で変更されてしまいます。

5.3 ファイル操作

参照 「コマンドリファレンス」/「運用・管理」/「ファイル操作」

○ ZMODEM で転送するファイルのサイズは 3MByte 以下にしてください。

○ USB メモリーに空き容量がない状態で、create autoboot コマンドを実行するとエラーメッセージが表示され、その後別の USB メモリーを使用しようとすると、正しくディレクトリーが読み取れません。エラーメッセージ出力後に別の USB メモリーを使う際は、一度本体を再起動してから使用してください。同一の USB メモリーを使用するには問題ありません。

○ cd コマンドにて USB メモリーを利用中に、USB メモリーを抜き、その後 USB メモリーを挿しなおすと、本製品が USB メモリーを認識しないことがあります。USB メモリーを抜く前には必ず、cd flash で USB メモリーの利用を中止してください。

○ USB メモリーを取り外した時のメッセージが Enter キーを入力するまで表示されません。

○ edit, mkdir, rmdir, show file, show file systems コマンドを使用して Apricorn 社の SecureUSB メモリー ASK-256-8GB/16GB/32GB 上のファイルにアクセスした場合、ASK-256-8GB/16GB/32GB 上のアクセス LED が点滅状態のままになることがあります。その場合は、「dir usb:/」のように、USB メモリーにアクセスする操作をもう一度行ってください。

○ Apricorn 社の SecureUSB メモリー ASK-256-8GB/16GB/32GB 使用時、カレントディレクトリーが USB メモリー上にある間は、ASK-256-8GB/16GB/32GB 上のアクセス LED が点滅状態のままになりますが、動作上の問題はありません。また、カレントディレクトリーを USB メモリー以外に移動すると点滅状態は解除されます。

○ Apricorn 社の SecureUSB メモリー ASK-256-8GB/16GB/32GB を装着している状態でシステムを再起動した場合、再起動時 SecureUSB メモリーの仕様によりロックがかかるため、再起動後に USB メモリーのセキュリティーを解除するための PIN コードを再度入力してください。

○ 2GByte 以上のファイルに対して、copy、delete、move コマンドで操作することはできません。dir コマンドでファイルの存在を確認することは可能です。

5.4 ユーザー認証

参照「コマンドリファレンス」/「運用・管理」/「ユーザー認証」

○ アクセスが許可されていないホスト / ユーザーから SSH でログインしようとした場合、コンソール上にデバッグメッセージが表示されます。

○ tacacs-server timeout コマンドで設定できるタイムアウト値の最大は 190 秒です。

○ CLI ログイン認証に TACACS+ を使用するとき、同時に使用できる仮想端末ポート（VTY）の数は 20 までとなります。また内部のユーザー認証データベースを使用するときは、同時に使用できる仮想端末ポート（VTY）の数は 33 までとなります。

○ TACACS+ 認証を使用して VCS マスターにログイン後、他のスタックメンバーにリモートログインしている最中に、ほかの TACACS+ セッションが同じユーザー名、パスワードでログインすると、以下のメッセージが出力されます。
・ You don't exist, go away!

○ CLI ログイン認証に TACACS+ サーバーを利用、かつ、特権パスワード（enable password）を設定している環境において、TACACS+ サーバーダウンにより装置本体のユーザー認証データベースで認証された権限 15 のローカルユーザーが enable コマンドを実行した場合、本来なら権限 15 のユーザーには要求されない特権パスワードの入力プロンプトが表示されます。その場合は任意の文字列を入力することで、特権 EXEC モードに移行できます。

○ TACACS+ サーバーを利用したコマンドアカウンティング（aaa accounting commands）有効時、end コマンドのログは TACACS+ サーバーに送信されません。

○ TACACS+ サーバーを利用した CLI ログインのアカウンティングにおいて、SSH 経由でログインしたユーザーのログアウト時に Stop メッセージを送信しません。

5.5 RADIUS クライアント

参照「コマンドリファレンス」/「運用・管理」/「RADIUS クライアント」

ローカル RADIUS サーバーに登録していない RADIUS クライアント（NAS）から、RADIUS Access-Request パケットを受信した場合、show radius local-server statistics コマンドで表示される Unknown NAS のカウンターがカウントアップしません。

5.6 RADIUS サーバー

参照「コマンドリファレンス」/「運用・管理」/「RADIUS サーバー」

○ USB メモリーを利用してローカル CA の証明書をダウンロードする際、USB メモリーにすでに同じ名前のローカル CA の証明書が入っていた場合、Overwrite usb:/rootca.cer? (y/n) と確認のメッセージが表示されますが、Y も N も入力できず、上書きできません。USB メモリーに入っているファイルを削除するか、ファイル名を変更してダウンロードを行ってください。

○ server auth-port コマンドによりローカル RADIUS サーバーの認証用 UDP ポート番号を 63998 以上に設定しようとすると、関連プロセスが再起動するログが出力されます。また、上記の UDP ポート番号を使用してポート認証を行うことができません。

○　ローカル RADIUS サーバーと 2 ステップ認証は併用できません。

○　ローカル RADIUS サーバーに登録するユーザー名の長さは 63 文字までにしてください。

5.7　ログ

参照「コマンドリファレンス」/「運用・管理」/「ログ」

○　保存するメッセージの最大量が log size コマンドで設定した値と異なります。

○　MSTP 有効時、多数のインターフェースが同時にアップまたはダウンし、ログメッセージが大量に発生した場合、すべてのログメッセージが Syslog サーバーに転送されない場合があります。

○　ターミナルモニターを有効にした後、VCS のバックアップメンバーにリモートログインを行いながら USB メモリーを抜き差しすると、ターミナルモニターのログが正しく表示されません。

○　no log buffered コマンドを入力してランタイムメモリー（RAM）へのログ出力を一度無効にした後、default log buffered コマンドを実行しても、ログ出力が再開しません。その場合は「log buffered」を実行することにより再開できます。

○　以下のログがコンソールに表示されないことがあります。
- Configuration update completed for portxxx
- Member x (xxxx.xxxx.xxxx) has become the Active Master

○　不揮発性メモリー（NVS）に出力するログメッセージのメッセージフィルターを追加した後、default log コマンドを使用して不揮発性メモリーのログ出力を初期値に戻しても、作成されたメッセージフィルターが削除されません。
メッセージフィルターは、log(filter) コマンドを no 形式で実行するか、本体を再起動すると削除されます。

○　（AT-x510-28GPX/AT-x510-52GPX のみ）起動時において、電源ユニットに関するログが不自然なタイミングで表示されます。また、2 つの電源ユニットがどちらも正しく動作しているにもかかわらず、一方についてのログしか表示されない場合があります。

5.8　トリガー

参照「コマンドリファレンス」/「運用・管理」/「トリガー」

トリガー設定時、script コマンドで指定したスクリプトファイルが存在しない場合、コンソールに出力されるメッセージ内のスクリプトファイルのパスが誤っています。

誤：

% Script /flash/script-3.scp does not exist. Please ensure it is created before

正：

% Script flash:/script-3.scp does not exist. Please ensure it is created before

また、スクリプトファイルが存在しないにもかかわらず前述のコマンドは入力できてしまうため、コンフィグに反映され、show trigger コマンドのスクリプト情報にもこのスクリプトファイルが表示されます。

5.9 LLDP

参照「コマンドリファレンス」/「運用・管理」/「LLDP」

○ VCS 構成時、LLDP MIB の lldpPortConfigAdminStatus は未サポートです。

○ トランクポートに LLDP を設定すると、show lldp neighbors interface コマンドで表示される LLDP 有効ポートが正しく表示されません。

5.10 SNMP

参照「コマンドリファレンス」/「運用・管理」/「SNMP」

○ LACP を使用しトランクグループを作成した際、対向機器の SNMP マネージャーで linkDown トラップを受信できない場合があります。送信先ホストの設定をする際、通知メッセージの形式で informs を指定すると informs パケットが受信できます。

○ VCS 構成のシャーシに GetNext Request を送信すると、SNMP が「no such object」と応答することがあります。

○ SNMP MIB で、ifHCInUcastPkts と ifHCOutUcastPkts の値が正しくありません。それぞれ、ユニキャストパケットの受信数と送信数を示すはずですが、ブロードキャスト / マルチキャストパケットもカウントされてしまいます。

○ snmp-server enable trap コマンドは、省略せずに入力してください。省略した場合、実行できない、または、コンソールの表示が乱れることがあります。

○ atFilev2FileViewerName を利用する場合は、ファイルシステム上に 112 文字以上のファイル名を持つファイルが存在しないことを確認してください。

○ SNMP マネージャー上から機器の RMON エントリーを作成するとエラーが発生し、エントリーが作成されない場合があります。

5.11 sFlow

参照「コマンドリファレンス」/「運用・管理」/「sFlow」

○ sflow collector コマンドで sflow の UDP ポートを設定したとき、コンフィグに反映されず、保存、再起動で初期設定に戻ってしまいます。再起動した場合は、再度設定してください。SNMP マネージャーから設定した場合も同様です。

○ sFlow が有効なインターフェースで VLAN タグがついたパケットを受信したとき、ingress 方向のサンプリング情報に VLAN タグ情報が付与されません。

○ sFlow MIB の sFlowFsReceiver と sFlowCpReceiver の値を変更後、初期値に戻すためには sFlow を無効にする必要があります。

5.12 NTP

参照「コマンドリファレンス」/「運用・管理」/「NTP」

○ 実際には NTP サーバーと時刻同期が取れていない状態でも、show ntp associations コマンド上では同期済みと表示される場合があります。

○ NTP を使用していると、以下のログが出力されますが、動作には問題ありません。
- frequency error 501 PPM exceeds tolerance 500 PPM

○ NTP を設定していないときでも、NTP カウンターがカウントアップします。

○ すでに NTP サーバーが設定されている状態で、別のサーバーに設定を変更した場合、一度設定を削除した後、新規に設定を追加してください。削除せずに変更した場合、正しく同期しない場合があります。

○ 初期設定時など、NTP を設定していない状態で show ntp status コマンドを入力すると、NTP サーバーと同期していることを示す以下のようなメッセージが表示されます。
- Clock is synchronized, stratum 0, actual frequency is 0.000PPM, presicion is 2

○ show ntp association detail コマンドの org time および xmt time の表示が、NTP による同期の有無にかかわらず、「06:28:16.000 UTC Thu Feb 7 2036」を示します。これは表示だけの問題で、システムの時計の動作には影響しません。

○ NTPv4 を使用している場合、ntp master コマンドによる NTP 階層レベル（Stratum）の設定と NTP サーバーによる時刻の取得を併用すると、NTP サーバーによって自動決定される階層レベルが優先されます。

○ DNS サーバーを複数登録（ip name-server）している場合、NTP サーバーの追加コマンド（ntp server）を実行すると、プロンプトが戻るまで 1 分以上かかる場合があります。

5.13 端末設定

参照「コマンドリファレンス」/「運用・管理」/「端末設定」

○ clear line console コマンドを実行すると、他の VCS メンバー上のコンソールで接続しているユーザーのセッションも切断されます。

○ コンソールターミナルおよび仮想端末における 1 画面当たり表示行数は、実際のコンソールターミナルや仮想端末に表示できる行数より小さい値に設定してください。

5.14 Telnet

参照「コマンドリファレンス」/「運用・管理」/「Telnet」

○ 本製品から他の機器に Telnet で接続しているとき、次のようなメッセージが表示されます。
- No entry for terminal type "network";
- using vt100 terminal settings.

○ 非特権モードでホスト名を使用して、Telnet 経由でリモートデバイスにログインする場合は、ドメイン名まで指定してください。

5.15 インターフェース

参照「コマンドリファレンス」/「インターフェース」

○ show interface コマンドで表示される dropped カウンターがカウントされません。show platform port counters コマンドの ifInDiscards カウンターで確認してください。

○ IPv6 アドレスを持つインターフェースに show interface コマンドを入力した際の結果に、実際のホップリミットの値が表示されません。

5.16 フローコントロール

参照「コマンドリファレンス」/「インターフェース」/「スイッチポート」

○ 10G ポートでは、show flowcontrol interface コマンドの RxPause カウンターが正しく表示されません。

○ 通信速度をオートネゴシエーションで決定しているとき、show flowcontrol interface コマンドで確認できる oper の状態が on になると、そのポートがリンクダウンした後も、表示が更新されません。これは表示のみの問題であり、動作に影響はありません。

○ フローコントロールとバックプレッシャーを同一ポートに設定し、フローコントロールを無効にすると、バックプレッシャーが動作しなくなります。フローコントロールとバックプレッシャーを同一ポートに設定しないでください。

○ 実際に送信した Pause フレームの数に対して、ポートカウンターの送信数が正しくカウントされません。これは表示のみの問題であり、動作に影響はありません。

5.17 ポートセキュリティー

参照「コマンドリファレンス」/「インターフェース」/「スイッチポート」

○ ジャンボフレームとポートセキュリティーは併用できません。

○ ポートセキュリティーによって学習された MAC アドレスをエージアウトしないよう設定し、ポートセキュリティーの不正パケット受信時の動作を指定している場合、ポートセキュリティーを無効にしてもスタティック MAC アドレスがコンフィグに残ったままになります。コンフィグに残ってしまったスタティック MAC アドレスは、no mac address-table static または、clear mac address-table コマンドで削除してください。

○ ポートセキュリティーにおいて、不正パケット受信時の動作を shutdown に設定している状態で、ポートセキュリティーを無効にすると、ログが正しく出力されず、show interface status コマンドでインターフェースのステータスが正しく表示されません。shutdown コマンドでインターフェースを無効にし、その後有効にすることで正しく表示されます。

5.18 パケットストームプロテクション

参照「コマンドリファレンス」/「インターフェース」/「スイッチポート」

リンク速度の異なるポートが混在する環境において、高速なポートにパケットストームプロテクションの設定を行った場合、高速なポートから低速なポートへの転送レートは、パケットストームプロテクションの設定値よりも低くなります。

5.19 ループガード

参照「コマンドリファレンス」/「インターフェース」/「スイッチポート」

○ LDF 検出機能により、ループを検出した VLAN のポートが無効化されている場合、switchport enable vlan コマンドを VID を指定せずに実行しても、無効化されている VLAN のポートは有効になりません。LDF 検出機能により無効化されている VLAN のポートを有効にするには、switchport enable vlan コマンドを VID を指定して実行してください。

○ LDF 送信間隔（loop-protection コマンドの ldf-interval パラメーター）を最小値の 1 秒に設定する場合、ループ検出時の動作持続時間（loop-protection timeout コマンド）は 2 秒以上に設定してください（初期値は 7 秒）。

○ 本来、LDF 機能はアクセスリストのエントリーに空きがない場合には使用できませんが、アクセスリストのエントリーに空きがない場合でも、loop-protection loop-detect コマンドを 1 回入力し、エラーメッセージが表示された後に、再度同じコマンドを入力すると、コマンドが実行されてしまいます。
また、loop-protection loop-detect コマンドを 1 回入力し、エラーメッセージが表示された後に、当該のポートからアクセスリストのエントリーを削除すると、アクセスリストの登録数と最大数が正しく表示されなくなります。

○ MAC アドレススラッシング検出時の動作に learn-disable アクションを設定しているとき、MAC アドレススラッシング検出後、MAC アドレスの学習が停止されないことがあります。

○ MAC アドレススラッシングプロテクション設定時、ループを検出したすべてのポートが、設定した動作を行います。

○ MAC アドレススラッシングプロテクションにおいて、vlan-disable、link-down アクション実行時のログメッセージに誤りがありますので、下記のとおり読み替えてください。
[vlan-disable の場合]
誤：Thrash: Loop Protection has disabled "port" on ifindex XXXX vlan X
正：Thrash: Loop Protection has disabled "VLAN" on ifindex XXXX vlan X

[link-down の場合]
誤：Thrash: Loop Protection has disabled "port" on ifindex XXXX
正：Thrash: Loop Protection has disabled "port-link" on ifindex XXXX

○　タグ付きポートで LDF 検出の vlan-disable アクション（初期値）を使用する場合は、該当ポートのネイティブ VLAN をなしに設定してください（switchport trunk native vlan none）。

5.20 ポートミラーリング

参照「コマンドリファレンス」/「インターフェース」/「スイッチポート」

複数ポートにインターフェースモードのコマンドを発行するときは、interface コマンドで対象ポートを指定するときに、通常ポートとして使用できないミラーポートを含めないようにしてください。ミラーポートを含めた場合、一部のポートに設定が反映されなかったり、エラーメッセージが重複して表示されたりすることがあります。

5.21 リンクアグリゲーション（IEEE 802.3ad）

参照「コマンドリファレンス」/「インターフェース」/「リンクアグリゲーション」

○　ポート認証と LACP を同一ポートで併用することはできません。認証ポートではスタティックチャンネルグループ（手動設定のトランクグループ）を設定するようにしてください。

○　スタティックチャンネルグループの対向機器の先に SNMP マネージャーが接続されている場合、スタティックチャンネルグループのメンバーポートをリンクアップした際、対向機器のリンクアップトラップが SNMP マネージャーに送信されないことがあります。

○　トランクグループ（saX, poX）に対して egress-rate-limit コマンドを実行した場合、送信レート上限値はトランクグループ全体に対してではなく、メンバーポート単位で適用されます。またこのとき、ランニングコンフィグ上でもトランクグループではなくメンバーポートに対する設定に変換されます（CLI からメンバーポートに対して同コマンドを実行するとエラーになりますが、スタートアップコンフィグから読み込んだときはエラーになりません）。

○　スタティックチャンネルグループ（手動設定のトランクグループ）において、shutdown コマンドによって無効にしていたポートに対して no shutdown コマンドを入力しても、ポートが有効にならないことがあります。
この場合は、再度 shutdown コマンド、no shutdown コマンドを入力してください。

○　スタティックチャンネルグループのインターフェースを shutdown コマンドにより無効に設定した後、リンクアップしているポートをそのスタティックチャンネルグループに追加すると、該当するインターフェースが再び有効になります。

○　マルチキャストパケットの受信中に LACP チャンネルグループのメンバーポートをリンクダウンさせると次のようなログメッセージが出力されますが、動作には影響ありません。

- 2012 Nov 2 02:22:47 user.err xXXX-1 HSL[572]: HSL: ERROR: Can't find multicast
- FDB entry : Port port1.0.3 mac (0100.5e00.0002) VID 20

○ show interface コマンドで表示される poX インターフェース（LACP チャンネルグループ）の input packets 欄と output packets 欄の値には、リンクダウンしているメンバーポートの値が含まれません。
LACP チャンネルグループ全体の正確な値を確認するには、poX インターフェースではなく各メンバーポートのカウンターを参照してください。

○ LACP ポート上にエンハンストプライベート VLAN のセカンダリーポートを設定することは未サポートとなります。

○ リンクアグリゲーションを設定した状態で、[no] mac address-table acquire コマンドを実行すると、不要なログメッセージが出力されますが、MAC アドレステーブルの自動学習機能には影響ありません。

5.22 ポート認証

参照 「コマンドリファレンス」/「インターフェース」/「ポート認証」

○ EAP 透過機能で forward（受信した EAPOL パケットを VLAN に関係なくすべてのポートに転送する）に設定した場合、ポートミラーリングのソースポートからコピーされた EAPOL パケットとは別にミラーポートへ EAPOL パケットが転送されます。

○ dot1x port-control コマンドでポート認証を有効にしたときに自動的に入る dot1x control-direction の設定が no dot1x control-direction で削除できません。コンフィグ上から dot1x control-direction コマンドを削除する場合は、no dot1x port-control を使用してください。また、ポート認証が無効にも関わらずポートに dot1x control-direction の設定が残っている場合も no dot1x port-control で削除してください。

○ Supplicant の再認証間隔（reAuthPeriod）の初期値は 3600 秒ですが、2 回目の再送間隔は約 1800 秒と前回の再送間隔の約半分になります。一定間隔で再送する場合は、auth timeout reauth-period コマンドで初期値以外の値を設定してください。

○ VCS とリンクアグリゲーション併用時、トランクポートで認証を行った後、Supplicant 宛てのパケットを VCS のスレーブで受信すると不必要なログメッセージが出力されます。

○ ローミング認証有効時、同時に多数の Supplicant のポート移動を行うと、再認証が発生する場合があります。

○ スタティックチャンネルグループ内にゲスト VLAN に所属している Supplicant がいると、そのトランクポートのコンフィグに switchport access vlan の設定が追加されてしまいます。チャンネルグループを削除しても switchport access vlan の設定は残るので、先に switchport access vlan の設定を削除してからチャンネルグループを削除してください。

○ 802.1X 認証の Supplicant がログオフしても、ステータスが Connecting になりません。

○ Web 認証において、一度プロミスキャスモードに設定すると、その後インターセプトモードに変更しても、プロミスキャスモード設定時と同様に、動作します。

インターセプトモードに設定を変更後、コンフィグを保存し、再起動した場合は、インターセプトモードとして動作します。

○ 802.1X 認証において、認証を 3 台以上の RADIUS サーバーにて行う場合、はじめの 2 台の RADIUS サーバーにて認証に失敗した際、Authenticator から 3 台目の RADIUS サーバーに Access-Request が送信されません。

○ 認証済みポートが認証を解除されても、マルチキャストトラフィックが該当ポートに転送され続ける場合があります。

○ バージョン **5.4.3-2.5** より前のファームウェアにおいて、一度でも Web 認証サーバー（HTTPS）用の独自 SSL 証明書をインストール（copy xxxxx web-auth-https-file）したことがある場合、独自証明書を削除して、Web 認証サーバーにシステム付属の証明書を使わせるには、次の手順を実行してください。

1. 独自にインストールした SSL 証明書を削除する。
awplus# erase web-auth-https-file

2. HTTP サービスを再起動する。
awplus(config)# no service http
awplus(config)# service http

またはシステムを再起動する（※ 未保存の設定がある場合は再起動前に保存してください）。
awplus# reboot

○ Single-Host モードの 802.1X 認証ポートに auth supplicant-mac コマンドを設定する場合は、該当ポートに複数の Supplicant を接続しないでください。

○ MAC ベース認証と Web 認証の 2 ステップ認証を利用する際は、認証スイッチと RADIUS サーバーとの間で使用する認証方式を、それぞれ別の方式に設定してください。

○ 認証ポートが MAC 認証、Web 認証を併用しており、かつ直接サプリカントの Linkup/Down を検知しない環境にて、一度 Web 認証に失敗した後、サプリカントが DHCP の再取得を実施すると、その後 MAC 認証が実施されません。

○ 802.1X 認証と Web 認証の 2 ステップ認証機能利用時に、ローカル RADIUS サーバーは使用できません。また、2 ステップ認証で ローカル RADIUS サーバー以外の RADIUS サーバーを使用するときは、認証スイッチと RADIUS サーバーとの間で使用する認証方式を、802.1X 認証と Web 認証でそれぞれ別の方式に設定してください。

○ Web 認証と MAC ベース認証 /802.1X 認証の併用時に、プロミスキャスモードとダイナミック VLAN を使用する場合は、Supplicant のデフォルトゲートウェイとして本製品（Authenticator）を指定しないでください。

○ VCS とダイナミック VLAN を併用している際、マスター切り替えが二回発生すると show auth-mac コマンドで表示される VLAN ID が VCS マスターと VCS スレーブで異なった値になります。これは表示だけの問題であり、動作には影響ありません。

5.23 Power over Ethernet（AT-x510-28GPX、AT-x510-52GPX、AT-IX5-28GPX のみ）

参照「コマンドリファレンス」/「インターフェース」/「Power over Ethernet」

○ PoE に対応した機器（AT-x510-28GPX, AT-x510-52GPX）と PoE に対応していない機器（AT-x510-28GTX, AT-x510-52GTX, AT-x510-28GSX、AT-x510DP-52GTX）が混在した VCS 環境において、power-inline enable コマンドを入力すると、PoE に対応していない機器に対するエラーメッセージが表示されますが、一部の非 PoE ポートの分しか表示されません。

○ power-inline enable コマンドを no 形式で実行し、PoE 給電機能を無効に設定すると、本来、show power-inline コマンドの Oper の表示が「Disabled」と表示されるべきですが、受電機器が接続されたポートでは「Off」と表示されます。

○ PoE 電源の電力使用量が最大供給電力を上回った場合、show power-inline interface detail コマンドの Detection Status は「Denied」と表示されるべきですが、「Off」と表示されてしまいます。
同様に、ポートの出力電力が上限値を上回った場合、「Fault」と表示されるべきですが、「Off」と表示されてしまいます。

○ ポートの出力電力が上限値を上回った状態で数分間放置すると、実際に接続している受電機器の電力クラスと異なる電力クラスが表示される、または「n/a」と表示されることがあります。また、これに伴って Max も実際とは異なる値が表示されます。ポートの出力電力が上限値未満に戻ると、表示も回復します。

○ ポートの出力電力が上限値を上回った状態のとき、show power-inline の Oper の表示が、実際の「Fault（ポートの出力電力が上限値を上回ったために給電を停止している）」ではなく「Denied（PoE 電源の電力使用量が最大供給電力を上回ったために給電を停止している）」となることがあります。

○ （AT-IX5-28GPX のみ）プリスタンダード方式の受電機器を接続した場合、ポートがリンクアップしないことがあります。ポートがリンクアップしないときは、ケーブルの抜き差しを行ってください。

5.24 バーチャル LAN

参照「コマンドリファレンス」/「L2 スイッチング」/「バーチャル LAN」

○ vlan コマンドは数値とカンマ、ハイフンだけを受け付ける仕様ですが、指定値にこれら以外の文字が含まれていてもエラーになりません。このとき、意図した VLAN が作成されなかったり（例：「10,20」のつもりで「10.20」と誤入力すると「10」しか作成されない）、意図したのとは異なる VLAN が作成されたりする（例：「1001」のつもりで「100q」と誤入力すると「100」が作成される）場合がありますのでご注意ください。

○ 大量に VLAN を作成後、switchport trunk allowed vlan コマンドを except オプション付きで指定しトランクポートの設定を行うと、再起動することがあります。
switchport trunk allowed vlan コマンドを except オプション付きで指定するときには、VLAN 数を 700 以内にしてください。または、except オプションではなく、add または、all オプションを設定してください。

○ プライベート VLAN からプライマリー VLAN を削除する場合は、事前にプライマリー VLAN、セカンダリー VLAN ともに、プライベート VLAN の関連付けを解除してください。その後、プライマリー VLAN のみを削除、再作成し、改めてプライベート VLAN とプライマリー VLAN、セカンダリー VLAN の関連付けを行ってください。

○ エンハンストプライベート VLAN を設定したポートからプライベート VLAN 用ポートとしての設定を削除すると、該当のポートでパケットが転送できなくなります。プライベート VLAN 用ポートとしての設定を削除した後は、本製品を再起動してください。

○ ダブルタグ VLAN のプロバイダーポートをミラーリングした場合、platform vlan-stacking-tpid コマンドの設定にかかわらず、TPID は常に 8100 となります。

○ プライベート VLAN のプロミスキャスポートに手動設定のトランクグループ（スタティックチャンネルグループ）を設定した場合、再起動後、ホストポートへパケットが転送されません。
再起動後、プロミスキャスポートの設定を再入力すると、パケットが正常に転送されるようになります。

○ プライベート VLAN 設定時にアップリンク側のマッピングを複数設定した場合は、設定を保存して再起動を行ってください。

5.25 GVRP

参照「コマンドリファレンス」/「L2 スイッチング」/「GVRP」

学習する VLAN 情報が多い場合、GVRP を設定しているポートをダウンさせ、その後すぐにアップさせると、正常に VLAN 情報が学習できなくなります。GVRP を利用する際の最大 VLAN 数は、100 です。

5.26 スパニングツリープロトコル

参照「コマンドリファレンス」/「L2 スイッチング」/「スパニングツリープロトコル」

○ チャンネルグループを作成後に MSTP を有効にすると、FDB に学習した MAC アドレスがケーブルがリンクダウンしてもクリアされません。チャンネルグループを作成する前に MSTP を有効にしてください。

○ VCS と PIM-SM を併用している時、リブートローリングを行うと 20 秒程度のマルチキャストトラフィックの通信断が発生します。

5.27 イーサネットリングプロテクション（EPSR）

参照「コマンドリファレンス」/「L2 スイッチング」/「イーサネットリングプロテクション」

○ EPSR と GVRP の併用は未サポートになります。

○ EPSR とトンネルインターフェースの併用は未サポートになります。

5.28 DHCP Snooping

参照「コマンドリファレンス」/「L2 スイッチング」/「DHCP Snooping」

○ snmp-server enable trap コマンドで DHCP Snooping 関連のトラップを有効に設定しているとき、ip dhcp snooping violation コマンドでトラップを設定しようとすると、「SNMP trap for DHCP Snooping is disabled」というメッセージが表示され、トラップの設定が有効になりません。トラップを設定する場合は、ip dhcp snooping violation コマンド、snmp-server enable trap コマンドの順に入力してください。また、上記のエラーメッセージが表示された場合は、再度 snmp-server enable trap コマンドを入力することで、トラップの設定が有効になります。

○ ip dhcp snooping agent-option allow-untrusted コマンドを実行し、リレーエージェント情報オプション（オプションコード 82）を含む DHCP パケットの Untrusted ポートでの受信を有効（破棄しない）に設定しても、リレーエージェント情報オプションを含む DHCP パケットが破棄されます。

5.29 IP ルーティング

参照「コマンドリファレンス」/「IP ルーティング」

ループバックインターフェースに IP アドレスを設定した時、ループバックインターフェース宛のルートエントリーがハードウェアテーブルに登録されません。

5.30 経路制御

参照「コマンドリファレンス」/「IP ルーティング」/「経路制御」

maximum-paths コマンドを設定して、コストパスの最大値を変更しても有効になりません。

5.31 RIP（x510 シリーズのみ）

参照「コマンドリファレンス」/「IP ルーティング」/「経路制御（RIP）」

RIP 認証機能において、複数のパスワード（キーチェーン）を設定した時、送信される RIP パケットの中に含まれるパスワードは、1 番目に設定したパスワードのみになります。

5.32 OSPF（x510 シリーズのみ）

参照「コマンドリファレンス」/「IP ルーティング」/「経路制御（OSPF）」

○ 2 つのルーターの各々に同じ送信先アドレスとネクストホップを持つスタティックルートを設定し、External LSA の Forwarding address が Non-Zero になる設定をしたとき、優先度の低い（router ID の低い値を持つ）ルーターがグレースフルリスタートをさせると、優先度の低いルーターからの External LSA を登録してしまいます。不正な AS External LSA の情報を元にルート情報が作成されますが、経路は登録されていますので通信は可能です。

○ VRRP が動作する機器は、OSPF のエリア境界ルーター（ABR）に設定することはできません。
ABR でグレースフルリスタートが発生した後、隣接関係をダウンさせると、隣接関係を保持していたサブネットのサマリー LSA が削除されます。

○ OSPF において、代表ルーター（DR）として動作している時に clear ip ospf process コマンドを入力すると、隣接ルーターが DR に変更されます。

○ OSPF 使用時、グレースフルリスタート後や VCS のマスター切り替え後に show ip ospf route コマンドを実行すると、インターフェース経路の種別が通常の「C（Connected）」ではなく「O（OSPF）」と表示されます。これは表示だけの問題であり、通信には影響ありません。また、インターフェースのダウンや OSPF プロセスの再起動によって解消されます。

○ OSPF の経路フィルタリングにおいて、match metric コマンドを使った特定経路の破棄ができません。

○ OSPF で完全スタブエリア（area stub no-summary）に指定すると、本来そのエリア内にはデフォルトルートのみを通知するべきですが、各エリアへのルート情報（タイプ 3LSA）が通知されてしまいます。

5.33 ARP

参照「コマンドリファレンス」/「IP ルーティング」/「ARP」

マルチキャスト MAC アドレスをもつスタティック ARP エントリーを作成した後、それを削除してから arp-mac-disparity コマンドを有効にして、同一のエントリーをダイナミックに再学習させる場合は、設定後にコンフィグを保存して再起動してください。

5.34 VRRP

参照「コマンドリファレンス」/「IP ルーティング」/「VRRP」

VRRP において、バーチャル IP アドレスと同一ネットワークからの通信に対しては応答しますが、別のネットワークから自身のバーチャル IP アドレス宛ての通信には応答しません。

5.35 IPv6 ルーティング

参照「コマンドリファレンス」/「IPv6 ルーティング」

○ IPv6 アドレスを設定する際、不正なインターフェース ID が指定されてもエラーになりません。

○ 自身の IPv6 アドレス宛に ping を実行するとエラーメッセージが表示されます。

○ IPv6 において、インターフェース経路（直接経路）が 2 重に登録されることがあります。

○ IPv6 において、VLAN が削除されたとき、リンクローカルアドレスが IPv6 転送表から消えません。

○ ICMPv6 の宛先マルチキャストアドレスが MTU よりも大きい場合、Packet Too Big メッセージを出力しないため　正しく IPv6 経路 MTU 探索ができません。

○ フラグメントされた IPv6 Echo Request は利用できません。利用した場合 Duplicate パケットは正しく再構築されませんのでご注意ください。

5.36 6to4 トンネリング（x510 シリーズのみ）

参照「コマンドリファレンス」/「IPv6 ルーティング」/「IPv6 インターフェース」

6to4 のトンネリングが確立している状態で DSCP 値をダイナミックに変更すると、その後トンネリングの確立に失敗します。DSCP 値を変更する場合は、変更後の設定を保存後、機器を再起動してください。

5.37 OSPFv3（x510 シリーズのみ）

参照「コマンドリファレンス」/「IPv6 ルーティング」/「経路制御（OSPFv3）」

○ 動作中の機器に OSPFv3 の設定をした場合、OSPFv3 が動作する VLAN インターフェースが一度リンクアップしないと、show ipv6 ospf interface コマンドで、OSPFv3 インターフェースの情報が表示されません。設定後は、機器を再起動するか、VLAN インターフェースの所属ポートをリンクアップさせてください。

○ OSPFv3 使用時、passive-interface コマンドで指定するパッシブインターフェースには、実在するインターフェースのみを指定してください。

○ OSPFv3 Authentication の設定を変更した場合は、設定を保存後、再起動してください。

5.38 近隣探索

参照「コマンドリファレンス」/「IPv6 ルーティング」/「近隣探索」

イベントログ上に「Neighbor discovery has timed out on link eth1->5」のログメッセージが不要に表示されることがあります。これは表示上の問題であり通信には影響はありません。

5.39 PIM（x510 シリーズのみ）

参照「コマンドリファレンス」/「IP マルチキャスト」/「PIM」

○ PIM-DMv4 インターフェースをサポートリミット値まで設定した後、VLAN インターフェースから PIM-DMv4 の設定を削除し、別の VLAN インターフェースに PIM-DMv4 を設定しようとすると、下記のエラーが出力され、設定ができません。その場合は、設定を保存してから再起動してください。
% Maximum number of pim-dm interfaces reached

○ PIM-SSM の範囲外のマルチキャストアドレスを受信しても破棄しません。

○ SSM マッピング機能の設定を削除した場合は、設定保存後に再起動してください。

5.40 IGMP

参照「コマンドリファレンス」/「IP マルチキャスト」/「IGMP」

○ ip igmp static-group コマンドで source パラメーターを指定しても、指定した送信元 IP アドレス以外からのマルチキャストパケットも指定したポートにだけ送信してしまいます。

○ show ip igmp groups コマンドの表示結果に、IGMP を有効に設定していない VLAN が表示されることがあります。これは show ip igmp groups コマンドの表示だけの問題であり、動作に影響はありません。

○ IGMP プロキシーにおいて、下流インターフェースに指定している VLAN を無効にしても、上流インターフェースにグループ情報が残り続けます。

○ スタティックマルチキャストグループが登録されている状態で、該当のマルチキャストグループと同じグループアドレス宛ての Join メッセージを他のポートから受信すると、その後 Leave メッセージを受信しても、そのポートには該当マルチキャストグループ宛のマルチキャストパケットが転送されるようになります。

○ マルチキャストグループをスタティックに登録した後、登録したインターフェースにスタティックに登録してあるものと同じマルチキャストグループの参加、離脱が発生すると、マルチキャストグループがコンフィグから削除しても消せなくなります。
この場合は、マルチキャストグループにメンバーが参加した状態で ip igmp static-group コマンドを no 形式で実行するか、IGMP 機能を一旦無効にし、再度有効にすると、マルチキャストグループは正常に削除されます。

○ IGMP プロキシーは未サポートです

5.41 IGMP Snooping

参照「コマンドリファレンス」/「IP マルチキャスト」/「IGMP Snooping」

○ 空の Exclude リストを持つグループレコードが存在している状態で、同グループに対する Exclude リスト追加要求（BLOCK_OLD_SOURCES）を受信すると、それ以降該当グループがタイムアウトしたり、脱退メッセージ（CHANGE_TO_INCLUDE{}）を受信したりしても、該当グループが正しく削除されません。

○ IGMP Snooping が有効な状態で、一旦無効にし、再度有効にした場合、その後に受信する IGMP Report を全ポートにフラッディングします。
IGMP Snooping を再度有効にした後、clear ip igmp group コマンドを実行して全てのエントリーを消去することで回避できます。

○ Include リスト（送信元指定）付きのグループレコードが登録されている状態で、あるポートに接続された唯一のメンバーからグループ脱退要求を受信すると、そのポートには該当グループのマルチキャストトラフィックが転送されなくなりますが、他のポートで同じグループへの参加要求を受信すると、脱退要求によって転送のとまっていたポートでもマルチキャストの転送が再開されてしまいます（この転送は、脱退要求を受信したポートの Port Member list タイマーが満了するまで続きます）。

○ VLAN ID のみ異なる、未登録の IP マルチキャストトラフィックをタグ付きポートで受信すると、該当マルチキャストトラフィックは、受信ポートが所属するすべての VLAN でフラッディングされます。ただし、各 VLAN で該当マルチキャストグループのメンバーが登録されると、IGMP Snooping が正常に動作するようになり、フラッディングは行われなくなります。

○ IGMP Snooping をいったん無効にし、再度有効にする場合は、システムを再起動してください。

○ ダイナミック登録されたルーターポートを改めてスタティックに設定した場合、ダイナミック登録されてから一定時間が経過すると設定が削除されます。また、一定時間が経過するまでの間、コンフィグ上にはスタティック設定が表示されますが、ip igmp snooping mrouter interface コマンドを no 形式で実行しても、コンフィグから削除することができません。
ルーターポートをスタティックに設定する場合は、該当のポートがダイナミック登録されていないことを確認してください。

○ グローバルコンフィグモードの ip igmp snooping コマンド、インターフェースモードの ip igmp snooping コマンドのどちらか一方のみが実行されている状態では、不要なパケットが複製され出力されます。

○ IGMP Snooping の設定を無効で起動した場合、有効に変更しても、IGMP パケットが正しく転送されません。IGMP Snooping を無効から有効に設定変更した場合は、設定を保存し再起動してください。

5.42 PIM（x510 シリーズのみ）

参照 「コマンドリファレンス」/「IPv6 マルチキャスト」/「PIM」

○ PIMv6 使用時、PIMv6 インターフェースが最大まで設定されているとき、それらの VLAN の一つを削除しても、新たに VLAN インターフェースに PIMv6 を設定することができません。
VLAN インターフェースから PIMv6 の設定を削除してから、VLAN を削除してください。

○ VRRPv3 と PIM-SMv6 は併用できません。

5.43 MLD

参照 「コマンドリファレンス」/「IPv6 マルチキャスト」/「MLD」

○ MLDv2 において、グループエントリーがスタティック登録されている状態で、同じグループがダイナミックに登録され、待機時間が経過した時、ダイナミック登録されたエントリーとともに、スタティック登録されたエントリーもコンフィグから削除されます。

○ clear ipv6 mld コマンド実行時に「% No such Group-Rec found」というエラーメッセージが表示されることがありますが、コマンドの動作には問題ありません。

○ MLD パケットの Max Query Response Time フィールドの値が、本製品の設定の 1/100 の数値で送出されます。MLD をお使いの際は、ipv6 mld query-max-response-time コマンドでなるべく大きい値（最大値は 240）を設定してください。

5.44 MLD Snooping

参照「コマンドリファレンス」/「IPv6 マルチキャスト」/「MLD Snooping」

○ グローバルコンフィグモードの ipv6 mld snooping コマンド、インターフェースモードの ipv6 mld snooping コマンドのどちらか一方のみが実行されている状態では、不要なパケットが複製され出力されます。

○ MLD Snooping の設定を無効で起動した場合、有効に変更しても、MLD パケットが正しく転送されません。MLD Snooping を無効から有効に設定変更した場合は、設定を保存し再起動してください。

○ MLD Snooping の Report 抑制機能が有効なとき（初期設定は有効）、ルーターポートで受信した MLDv1 Report または Done メッセージを受信ポートから再送出してしまいます。これを回避するには、「no ipv6 mld snooping report-suppression」で Report 抑制機能を無効化してください。

○ MLD Snooping をいったん無効にし、再度有効にする場合は、システムを再起動してください。

5.45 アクセスリスト

参照「コマンドリファレンス」/「トラフィック制御」/「アクセスリスト」

ntp access-group コマンドによって NTP サービスに対するアクセス制御の設定を行う場合、ホストを許可（permit）する形式で標準 IP アクセスリストを作成していると、エントリーにマッチするホストのみでなく、マッチしないホストも時刻の同期を行うことができてしまいます。
標準 IP アクセスリストを作成する際、許可するホストを指定したあとに、すべてを拒否（deny any）するエントリーを追加してください。

5.46 ハードウェアパケットフィルター

参照「コマンドリファレンス」/「トラフィック制御」/「ハードウェアパケットフィルター」

IGMP パケットはハードウェアパケットフィルターでフィルタリングできません。

5.47 Quality of Service

参照「コマンドリファレンス」/「トラフィック制御」/「Quality of Service」

○ ポリシーベースルーティングのネクストホップの最大登録数は 127 件です。

○ QoS の match eth-format protocol コマンドで AppleTalk パケットを制御できません。

○ match dscp コマンドの設定を削除する際、no match dscp と入力するとエラーとなります。
no match ip-dscp コマンドを入力することで、設定を削除できます。

○ wrr-queue disable queue コマンドを設定している状態で no mls qos コマンドにより QoS 自体を無効にする場合は、先に no wrr-queue disable queue を実行してください。

○ QoS の送信スケジューリング方式（PQ、WRR）が混在するポートを手動設定のトランクグループ（スタティックチャンネルグループ）に設定した場合、ポート間の送信スケジュールが正しく同期されません。トランクグループを設定した場合は、個々のポートに同じ送信スケジュール方式を設定しなおしてください。

○ mls qos map cos-queue コマンドで cos-queue マップを変更していても、マルチキャストパケットの CPU 宛て送信キューが、デフォルトの cos-queue マップにしたがって決定される場合があります。これらのマルチキャストパケットを任意の CPU 宛て送信キューに振り分けるには、remark new-cos コマンドを使って該当パケットの内部 CoS 値を書き換えてください。その際、該当パケットに対しては、デフォルトの cos-queue マップが適用されることにご注意ください。

5.48 DNS リレー

参照「コマンドリファレンス」/「IP 付加機能」/「DNS リレー」

DNS のキャッシュサイズまたはタイムアウトの設定を変更すると、IPv6 DNS キャッシュエントリーが削除されます。

5.49 DHCP リレー

参照「コマンドリファレンス」/「IP 付加機能」/「DHCP リレー」

セカンダリー IP アドレスを設定したインターフェースで DHCP リレーを有効にした場合、セカンダリー IP アドレスが優先的に使用されます。

5.50 DHCPv6 サーバー

参照「コマンドリファレンス」/「IP 付加機能」/「DHCPv6 サーバー」

DHCPv6 サーバー機能において、動的に割り当てるアドレスの最終有効時間が infinite（無期限）の場合、IPv6 アドレスを配布しても、show コマンドに反映されません。

5.51 Ping ポーリング

参照「コマンドリファレンス」/「IP 付加機能」/「Ping ポーリング」

Ping ポーリング機能を一旦無効化してから再度有効化すると、プロセス終了を示す以下のようなログが表示されますが、動作に問題はありません。

・ init: network/ping-poll main process (13750) killed by HUP signal

5.52 アライドテレシスマネージメントフレームワーク（AMF）

参照「コマンドリファレンス」/「アライドテレシスマネージメントフレームワーク」

○ AMF クロスリンク、EPSR、VCS を使用した構成で、VCS メンバーがダウンし、復旧した際、復旧した VCS メンバーに接続されている AMF ノードが認識されません。
EPSR リング内では、AMF Node Depth 値が異なる AMF ノード同士は AMF リンクで接続してください。

○ VCS 構成において、スタックリンクに障害が発生し VCS メンバーが Disabled Master 状態になると、スタックリンクとレジリエンシーリンク以外のポートは無効化されますが、EPSR を併用している場合、show atmf nodes コマンドの結果には、Disabled Master 状態となり無効化されたポートに接続された AMF ノードが表示されてしまいます。
EPSR リング内では、AMF マスターからの距離（ホップ数）の異なる AMF ノード同士は、AMF クロスリンクではなく AMF リンクで接続してください。

○ AMF リンクとして使用しているスタティックチャンネルグループの設定や構成を変更する場合は、次に示す手順 A・B のいずれかにしたがってください。

[手順 A]
1. 該当スタティックチャンネルグループに対して shutdown を実行する。
2. 設定や構成を変更する。
3. 該当スタティックチャンネルグループに対して no shutdown を実行する。

[手順 B]
1. 該当ノード・対向ノードの該当スタティックチャンネルグループに対して no switchport atmf-link を実行する。
2. 設定や構成を変更する。
3. 該当ノード・対向ノードの該当スタティックチャンネルグループに対して switchport atmf-link を実行する。

○ リブートローリング機能でファームウェアバージョンを A から B に更新する場合、すでに対象ノードのフラッシュメモリー上にバージョン B のファームウェアイメージファイルが存在していると、ファームウェアの更新に失敗します。このような場合は、対象ノードから該当するファームウェアイメージファイルを削除してください。

○ AMF で使用するホスト名の最大文字数は 62 文字です。

○ AMF ネットワークにおいて、デバイスのホスト名は重複しないようにつけてください。大文字・小文字は区別できません。

○ AMF マスター上で atmf recover コマンドによってメンバーノードの内蔵フラッシュメモリーの復元を実行した場合、復元が完了しても、マスターノード上で完了を示すメッセージが出力されません。復元の完了は、対象ノードにおけるログ出力によって確認できます。

○ インターフェースに以下の手順で AMF 設定を行うと、show atmf links コマンドの ATMF State が Incompatible となります。ATMF State が Incompatible になった場合、インターフェースをダウン・アップさせると正しく表示されます。

1 AMF 設定
2 AMF 設定解除
3 スタティックチャンネルグループ設定
4 上記スタティックへ AMF 設定

5.53 バーチャルシャーシスタック（VCS）

参照「コマンドリファレンス」/「バーチャルシャーシスタック」

○ VCS バックアップメンバーが再加入中にコンフィグを変更すると、再加入したバックアップメンバーにコンフィグが反映されないことがあります。バックアップメンバーが加入中に設定の変更はしないでください。

○ まれに VCS マスター切り替え後の新マスターが、設定されているプライオリティー値に従わずに選定されることがあります。

○ VCS スレーブを交換する際、マスターとスタックケーブルで接続して電源をオンにした後、通常、スタック ID を変更し、AMF を有効に設定するため、2 回の再起動が必要になりますが、AMF ネットワークに所属後、コンフィグの同期に時間がかかり、コンフィグの同期後に以下のようなエラーメッセージが表示され、もう一度再起動を要求されます。

- Post startup check found the following errors:
- Processes not ready:
- authd bgpd epsrd irdpd lacpd lldpd mstpd ospf6d ospfd pdmd pim6d pimd ripd ripngd rmond sflowd vrrpd
- Timed out after 300 seconds
- Bootup failed, rebooting in 3 seconds.
- Do you wish to cancel the reboot? (y) :

○ LDF が検出され link-down アクションが実行されている間にループを解消し、VCS マスター切り替えが発生すると、LDF 検出時アクションが実行されたポートが設定時間経過後も復旧しません。
該当のポートにて shutdown コマンドを no 形式で実行すると、リンクが復旧します。

○ VCS と EPSR を併用する場合、reboot rolling コマンドを実行した際に約 1 分程度の通信断が発生する場合があります。

○ マスター切り替えが発生したとき、「Failed to delete 'manager'」というメッセージが表示されることがあります。これは表示だけの問題で動作には影響しません。

○ VCS 構成時、EPSR と IGMP を併用している場合、IGMP タイマーは初期値より短く設定しないでください。

○ VCS 構成時は PIM と RSTP を併用できません。

○ VCS グループのファームウェア自動同期は 2 台構成時のみサポートとなります。3 台以上で VCS を構成する場合は手動で同じファームウェアバージョンにそろえてください。

○ 同一ネットワーク上に複数の VCS グループが存在する場合は、バーチャル MAC アドレスの下位 12 ビットとして使用されるバーチャルシャーシ ID を、該当する VCS グループ間で重複しないように設定してください。バーチャルシャーシ ID の設定は、stack virtual-chassis-id コマンドで行います。また、VCS グループのバーチャルシャーシ ID は、show stack コマンドを detail オプション付きで実行したときに表示される「Virtual Chassis ID」欄で確認できます。

○ VCS 構成において、6to4 トンネリング使用中ローリングリブートを実施するとパケットが重複して送出されます。

○ VCS マスターにログインしている状態からスレーブにリモートログインし、スレーブ上で、show users コマンドを実行しても、VCS マスターのコンソールログインの情報が表示されないことがあります。一度、コンソールからログアウトすると正しく表示されるようになります。

○ VCS 構成においてログを出力しない再起動、またはカーネルリブートが発生した後、新規マスターの全ポートのリンクダウン・アップが一時的に発生します。

○ VCS 構成において HSL プロセスが異常終了した場合、新規マスターの全ポートのリンクダウン・アップが発生します。

6 マニュアルの補足・誤記訂正

最新マニュアル（取扱説明書、コマンドリファレンス）の補足事項および誤記訂正です。

6.1 Power over Ethernet

参照 「CentreCOM x510 シリーズ 取扱説明書」（Rev.C）44 ～ 45 ページ

取扱説明書（Rev.C）の 44 ～ 45 ページに power-inline max コマンド（インターフェースモード）の記述がありますが、同コマンドはサポート対象外のため使用しないでください。

6.2 VCS グループの構成

参照 「AT-x510DP-52GTX/AT-IX5-28GPX 取扱説明書」（Rev.A）21 ページ、53 ページ

取扱説明書（Rev.A）において、VCS グループ構成の説明に誤りがありましたので、下記のとおり訂正いたします。

誤：

VCS グループは同一機種のみで構成されるようにしてください。AT-x510DP-52GTX と AT-IX5-28GPX との混在や、他の VCS サポート製品との混在はできません。

正：

VCS グループは x510 シリーズ（AT-x510DP-52GTX を含む）のみ、または AT-IX5-28GPX 同士で構成されるようにしてください。x510 シリーズと AT-IX5-28GPX との混在や、他の VCS サポート製品との混在はできません。

6.3 定格入力電流値

参照 「AT-x510DP-52GTX/AT-IX5-28GPX 取扱説明書」（Rev.A）84 ページ

取扱説明書（Rev.A）において、AT-PWR800-70/AT-PWR250-70 の定格入力電流値に誤りがありましたので、下記のとおり訂正いたします。

誤：

AT-PWR800-70：12A
AT-PWR250-70：3.0A

正：

AT-PWR800-70：10A
AT-PWR250-70：5.0A

6.4 ループガード（LDF 検出）

参照「コマンドリファレンス」/「インターフェース」/「スイッチポート」

ファームウェアバージョン **5.4.3-0.1** のリリースノート（Rev.B）には、「LACP と LDF 検出は併用できません」とありますが、LACP と LDF 検出は問題なく併用できます。

6.5 電源ユニットの抜き差しについて

参照「AT-x510DP-52GTX/AT-IX5-28GPX 取扱説明書」(Rev.A) 39 ページ

電源ユニットを抜き差しする場合は、必ず抜き差しする電源ユニットの電源をオフにしてください。また、電源ユニットを抜き差しする場合は、電源ユニット LED が完全に消灯したことを確認してから、再度取り付けるようにしてください。

6.6 SecureUSB メモリー使用時の注意事項

参照「コマンドリファレンス」/「運用・管理」/「システム」

参照「コマンドリファレンス」/「運用・管理」/「ファイル操作」

○ Apricorn 社の SecureUSB メモリー ASK-256-8GB/16GB/32GB を装着している状態でシステムを再起動した場合、再起動時 SecureUSB メモリーの仕様によりロックがかかります。USB 内のファームウェアファイルを起動用ファームウェアに指定して、再起動しないでください。

○ Apricorn 社の SecureUSB メモリー ASK-256-8GB/16GB/32GB をロックがかかったまま本製品に挿入すると、デバイス認識のリトライと失敗を繰り返すログが約 3 分間出続けますが、正常なものです。

6.7 802.1X 認証と Web 認証の併用時の動作

参照「コマンドリファレンス」/「インターフェース」/「ポート認証」

2 ステップ認証のサポートにより、802.1X 認証と Web 認証を併用する場合の動作が v5.4.3-3.7 から変更になりました。

・v5.4.3-2.5 以前の動作

802.1X 認証と Web 認証併用時は、802.1X で認証に失敗すると認証プロセスが完了となっていました。

・v5.4.3-3.7 以降の動作

802.1X 認証と Web 認証併用時は、802.1X で認証に失敗すると Web 認証に移行し、Web 認証でも認証に失敗すると認証プロセスが完了になります。

6.8 スパニングツリープロトコル

参照 「コマンドリファレンス」/「L2 スイッチング」/「スパニングツリープロトコル」

片方向通信中に STP でトポロジーチェンジが発生した場合、宛先 MAC アドレスがエージアウトしない場合があります。片方向通信のみの環境では、RSTP または MSTP を使用してください。

6.9 フォワーディングデータベース

参照 「コマンドリファレンス」/「L2 スイッチング」/「フォワーディングデータベース」

登録されている MAC アドレス宛へ通信を転送している場合、エージングタイム経過後も該当アドレスが MAC テーブルから削除されません。

7 サポートリミット一覧

パフォーマンス	
VLAN 登録数	単体：4094 VCS：2000※1
MAC アドレス（FDB）登録数	単体：16K VCS：4K※2
IPv4 ホスト（ARP）登録数	単体：2K VCS：768※3
IPv4 ルート登録数	1K※4
リンクアグリゲーション	
グループ数（筐体あたり）	128※5
ポート数（グループあたり）	8
ハードウェアパケットフィルター	
登録数	240※6※7※8
認証端末数	
認証端末数（ポートあたり）	1K
認証端末数（装置あたり）	1K
マルチプルダイナミック VLAN（ポートあたり）	1K
マルチプルダイナミック VLAN（装置あたり）	1K
ローカル RADIUS サーバー	
ユーザー登録数	100
RADIUS クライアント（NAS）登録数	24
その他	
VRF-Lite インターフェース数	-
IPv4 マルチキャストルーティングインターフェース数	31

※ 表中では、K=1024
※1 VCS 構成時、VCS グループに設定する VLAN の数は 2000 個までをサポートします。
※2 VCS 構成時、フォワーディングデータベース（FDB）のエントリー数は 4K 個までサポートします。

※3 VCS 構成時、IPv4 ホスト登録数（ARP エントリー数）は最大で 768 個までサポートします。
※4 インターフェース経路、スタティック経路、ダイナミック経路など、各種経路情報を含めた登録数です。
※5 スタティックチャンネルグループは 96 グループ、LACP は 32 グループ設定可能。合わせて 128 グループをサポートします。
※6 アクセスリストのエントリー数を示します。
※7 1 ポートにのみ設定した場合の最大数。エントリーの消費量はルール数やポート数に依存します。
※8 ユーザー設定とは別に、アクセスリストを使用する機能を有効化した場合に消費されるエントリーを含みます。

8　未サポート機能（コマンド）

最新のコマンドリファレンスに記載されていない機能、コマンドはサポート対象外ですので、あらかじめご了承ください。最新マニュアルの入手先については、次節「最新マニュアルについて」をご覧ください。

9　最新マニュアルについて

最新の取扱説明書「CentreCOM x510 シリーズ 取扱説明書」（613-001684 Rev.C）、「AT-x510DP-52GTX/AT-IX5-28GPX 取扱説明書」（613-001836 Rev.A）、コマンドリファレンス「CentreCOM x510 シリーズ コマンドリファレンス」（613-001763 Rev.F）は弊社ホームページに掲載されています。

なお、VCS の設定、運用に関する情報は、別紙「CentreCOM x510 シリーズ VCS 設定 / 運用マニュアル」に掲載しておりましたが、「CentreCOM x510 シリーズ コマンドリファレンス」（613-001763 Rev.B）以降、コマンドリファレンスに合わせて掲載しております。

本リリースノートは、これらの最新マニュアルに対応した内容になっていますので、お手持ちのマニュアルが上記のものでない場合は、弊社ホームページで最新の情報をご覧ください。

http://www.allied-telesis.co.jp/